RISCS

Research Institute in Science of Cyber Security

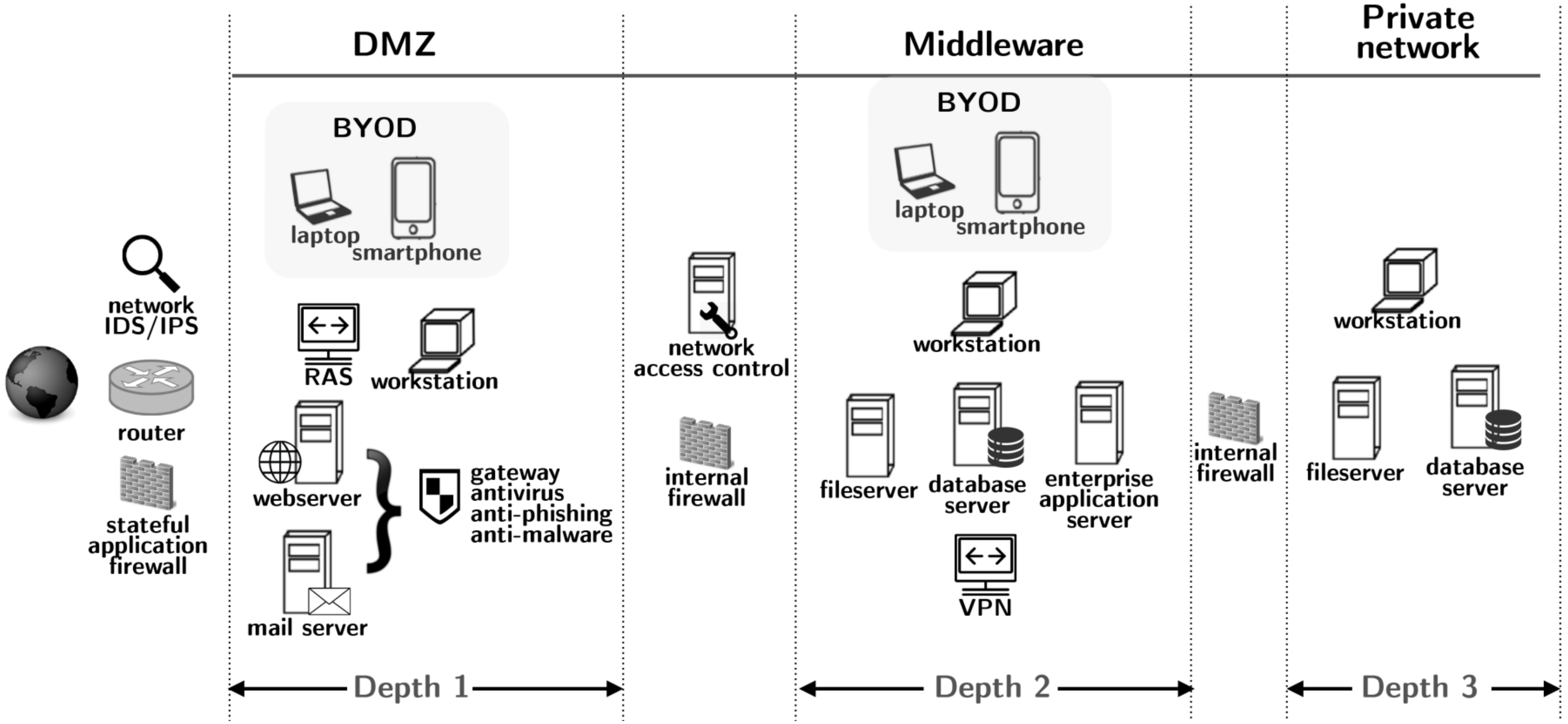
Imperial College London

Queen Mary University of London

Cyber Security Games and Investment: A Decision Support Approach

Emmanouil Panaousis
Andrew Fielder
Pasquale Malacaria
Chris Hankin
Fabrizio Smeraldi

Concepts (I)



- **Target:**
  - *Vulnerability*: The particular attack method for accessing the system
  - *Depth*: The network location of the data assets that will be compromised

Concepts (II)

- **Risk:** The perceived impact of a successful attack against targets at a given depth

- **Control:** The method for mitigating certain attacks
  - *Level*: The Degree to which a control is implemented
  - *Mitigation*: The amount of damage that is expected to be stopped by implementing this control
  - *Direct Cost*: The cost to implement and maintain a control
  - *Indirect Cost*: Costs related to the implementation of a control not seen as direct implementation or maintenance costs

- **Organisational Profile**: Characteristics unique to the Company or organisation, that dictate how they perceive aspects of their concerns outside of technical knowledge.

Concepts (III)

- **Risk**
  - Value of Data Loss – The cost of the data loss to the organisation
  - Business Disruption – The reduction in company functionality during recovery
  - Reputational Loss – Any loss in company standing from a successful attack
- **Threat**
  - Prevalence – The number of times the weakness is found in the system
  - Attack Frequency – The number of times someone actually tries to exploit it
  - Ease of Detection – A measure of the computational cost of the attack discovery process.
  - Attacker Awareness - Measures whether the average adversary would know that a malicious script is for sale
- **Indirect Cost**
  - System Performance – Reduction is system speed as a result of the control
  - Morale Cost – Productivity loss or additional security risks from users
  - Retraining Cost – Aspects of the control that require staff retraining
- **Mitigation**
  - The amount of protection a control provides to a given target

Game Theoretic Formulation (I)

- **Control Games –** All sub-games of a single control identifying the best strategy for each possible level.

- **Control Sub-Game –** The analysis of each possible combination of levels of a single control up to the maximum level denoted by the sub-game.

- **Representation**
  - Two Player, Zero Sum Game

$$U_{\mathcal{D}}(p_{jl}, \langle v_z, d\rangle) := \textsc{Risks} \times \textsc{Threat} \times (1 - \textsc{Mitigation}) + \textsc{Ind\_Costs}$$

$$Q^{\star}_{j\lambda} = \arg\max_{Q_{j\lambda}} \min_{H_{j\lambda}} U_{\mathcal{D}}(Q_{j\lambda}, H_{j\lambda}), \ \ \textit{and} \ \ H^{\star}_{j\lambda} = \arg\max_{H_{j\lambda}} \min_{Q_{j\lambda}} U_{\mathcal{A}}(Q_{j\lambda}, H_{j\lambda})$$

Game Theoretic Formulation (II)

Mixed Strategy

- A plan for the implementation of a control given a maximum level
- Applies a control in a proportional or probabilistic manner
  - Proportional – Proportion of employees who have the control implemented for them
  - Probabilistic – Probability that an action will take place with a certain frequency

"…we consider a security control related to password policy, and its 5 different implementation levels i.e. [0, 1, 2, 3, 4] where, for instance, level 4 corresponds to strong passwords that must change monthly. We also consider an organization with 1,000 employees among which 90 are senior managers (SM), 10 senior system administrators (SSA) and 900 other employees (OE) lower in hierarchy than SM and SSA. We imply that the level of each class of users is determined by the importance of data their accounts have access to.
A mixed strategy akin to cybersecurity plan ***[0, 0, 0.7, 0, 0.3]*** *partially says to implement level 4 of the control for SM and SSA who are 10% of the organization employees. Therefore there is a remaining 20% of employees that can implement the control at level 4."*

Optimisation (I)

- The Control Games focus on each control in isolation, the optimisation aims to show the result of combining controls to produce the best overall cybersecurity plan for an organisation.

- **Representation –** 0-1 Multiple Choice Multi-Objective Knapsack
  - 0-1 – A single control sub-game must be chosen in it's entirety
  - Multiple Choice – For each control only a single control sub-game may be selected.
  - Multi-Objective – Each target will be affected differently, so we define each as an objective to be optimised .
  - Knapsack Problem – Aims to build a plan for implementing different controls, similar to a classic Knapsack Problem

- **Direct Costs**
  - Capital Cost – The cost of implementing the control
  - Labour Cost – The cost of maintaining the control

Optimisation (II)

Maximises the minimum amount of damage seen across each target. So that the best solution (given by max) takes the value of min, which is the target that has the lowest overall cumulative benefit.

$$\max_{\mathcal{I}} \min_{t_i} \{1 - \sum_{j=1}^{N} \sum_{\lambda=0}^{\mathcal{L}} b_{j\lambda}(t_i) x_{j\lambda}\} \, \gamma_i$$

$$\textit{subject to} \sum_{j=1}^{N} \sum_{\lambda=0}^{\mathcal{L}} \omega_{j\lambda} x_{j\lambda} \leq B \ \textit{and} \ \sum_{\lambda=0}^{\mathcal{L}} x_{j\lambda} = 1, \ x_{j\lambda} \in \ \{0,1\}, \forall j = 1, \ldots, N$$

This condition is the budget constraint, where we consider if the control is used in the x term (either 0 or 1) and the cost of implementing it in the w.

This condition itentifies that for each of the N controls that only a single sub game solution can be (and must be) selected. Such that although they can only take a value of 0 or 1, the sum must equal 1, ensuring that a valid solution must select one sub game solution at level 1 and all others at level 0.

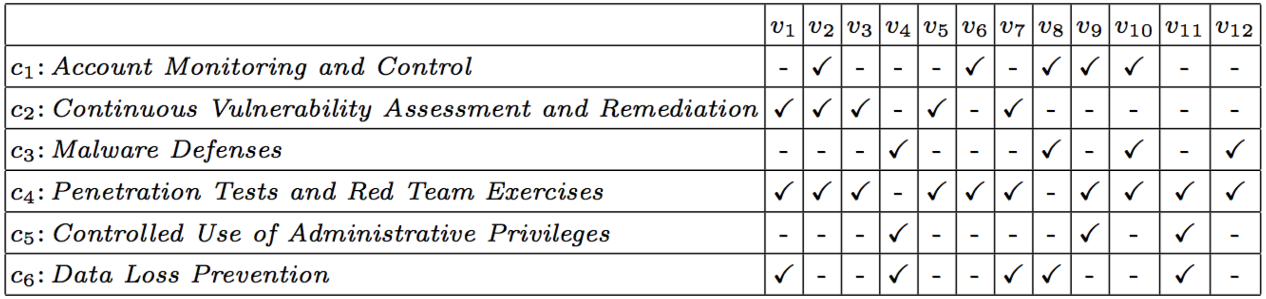
Case Study (I)

Overview

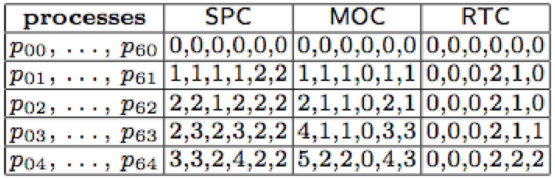
- An SME of approximately 30 People, with a network containing 3 depths
- Attackers using “Commodity Attacks”
- 6 Controls at 5 different levels, 12 Vulnerabilities at each of the 3 depths

Controls

- Taken from “Council on Cybersecurity: The critical security controls for effective cyber defence[1]”
- Two Kinds of Mitigation
  - Depth Based – Higher levels will implement controls at depths with lower valued data
  - Frequency Based – Higher levels of control implementation will implement aspects of the control more frequently



	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}
c_1: *Account Monitoring and Control*	-	✓	-	-	-	✓	-	✓	✓	✓	-	-
c_2: *Continuous Vulnerability Assessment and Remediation*	✓	✓	✓	-	✓	-	✓	-	-	-	-	-
c_3: *Malware Defenses*	-	-	-	✓	-	-	-	✓	-	✓	-	✓
c_4: *Penetration Tests and Red Team Exercises*	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	✓
c_5: *Controlled Use of Administrative Privileges*	-	-	-	✓	-	-	-	-	✓	-	✓	-
c_6: *Data Loss Prevention*	✓	-	-	✓	-	-	✓	✓	-	-	✓	-



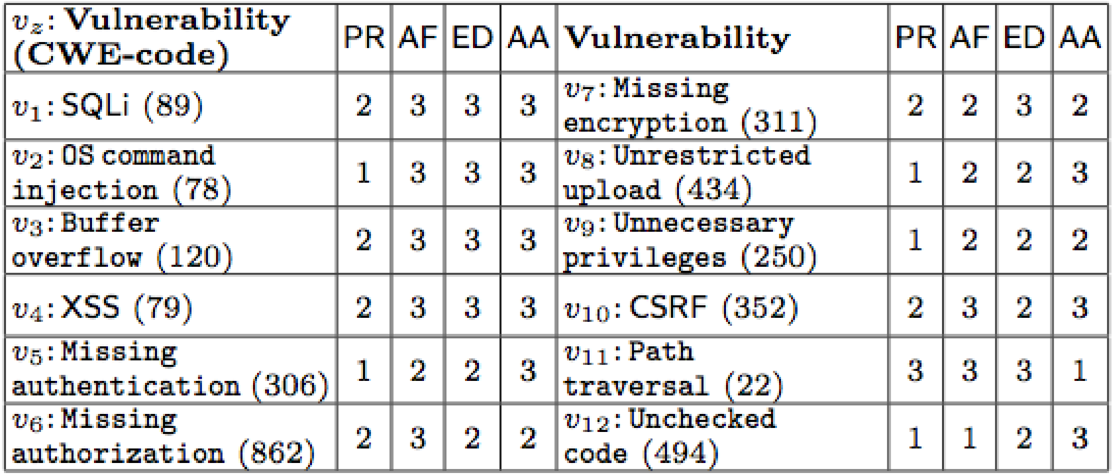
processes	SPC	MOC	RTC
$p_{00}, \ldots, p_{60}$	0,0,0,0,0,0	0,0,0,0,0,0	0,0,0,0,0,0
$p_{01}, \ldots, p_{61}$	1,1,1,1,2,2	1,1,1,0,1,1	0,0,0,2,1,0
$p_{02}, \ldots, p_{62}$	2,2,1,2,2,2	2,1,1,0,2,1	0,0,0,2,1,0
$p_{03}, \ldots, p_{63}$	2,3,2,3,2,2	4,1,1,0,3,3	0,0,0,2,1,1
$p_{04}, \ldots, p_{64}$	3,3,2,4,2,2	5,2,2,0,4,3	0,0,0,2,2,2

[1] http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf

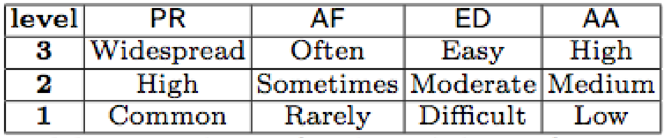
Case Study (II)

Vulnerabilities

- 12 Vulnerabilities taken from “CWE: 2011 CWE/SANS Top 25 Most Dangerous Software Errors.”



v_z: Vulnerability (CWE-code)	PR	AF	ED	AA	Vulnerability	PR	AF	ED	AA
v_1: SQLi (89)	2	3	3	3	v_7: Missing encryption (311)	2	2	3	2
v_2: OS command injection (78)	1	3	3	3	v_8: Unrestricted upload (434)	1	2	2	3
v_3: Buffer overflow (120)	2	3	3	3	v_9: Unnecessary privileges (250)	1	2	2	2
v_4: XSS (79)	2	3	3	3	v_{10}: CSRF (352)	2	3	2	3
v_5: Missing authentication (306)	1	2	2	3	v_{11}: Path traversal (22)	3	3	3	1
v_6: Missing authorization (862)	2	3	2	2	v_{12}: Unchecked code (494)	1	1	2	3



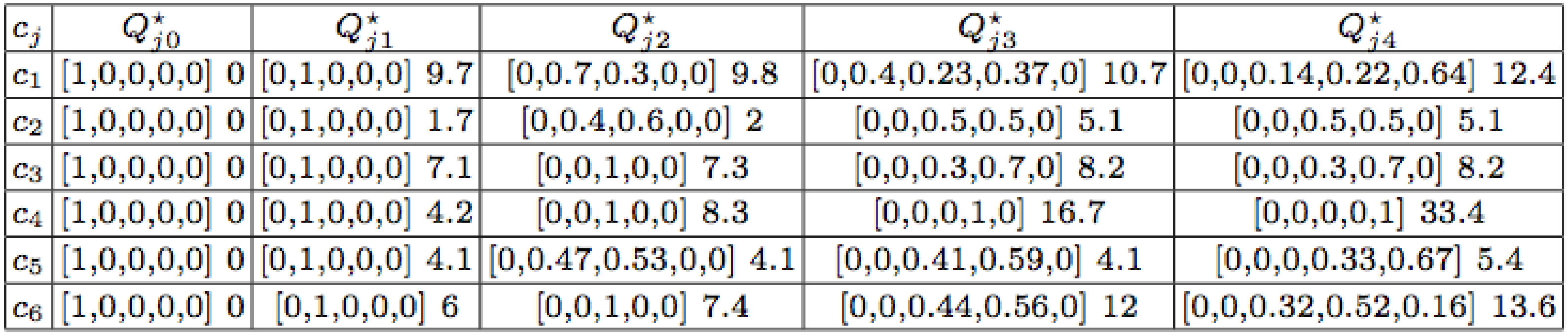
level	PR	AF	ED	AA
3	Widespread	Often	Easy	High
2	High	Sometimes	Moderate	Medium
1	Common	Rarely	Difficult	Low

[1] http://cwe.mitre.org/top25/

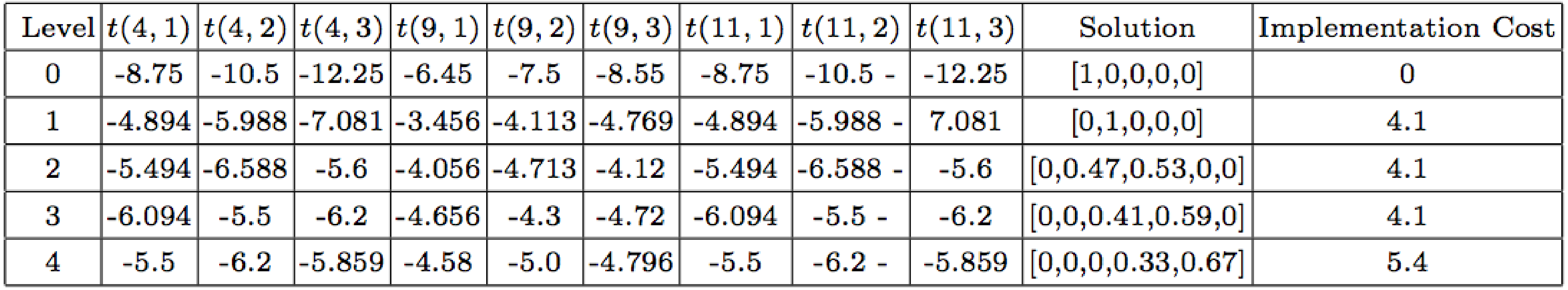
Results (I)

Game Results

- Results from the 5 Control Games and their associated levelised direct costs



c_j	$Q^\star_{j0}$	$Q^\star_{j1}$	$Q^\star_{j2}$	$Q^\star_{j3}$	$Q^\star_{j4}$
c_1	[1,0,0,0,0] 0	[0,1,0,0,0] 9.7	[0,0.7,0.3,0,0] 9.8	[0,0.4,0.23,0.37,0] 10.7	[0,0,0.14,0.22,0.64] 12.4
c_2	[1,0,0,0,0] 0	[0,1,0,0,0] 1.7	[0,0.4,0.6,0,0] 2	[0,0,0.5,0.5,0] 5.1	[0,0,0.5,0.5,0] 5.1
c_3	[1,0,0,0,0] 0	[0,1,0,0,0] 7.1	[0,0,1,0,0] 7.3	[0,0,0.3,0.7,0] 8.2	[0,0,0.3,0.7,0] 8.2
c_4	[1,0,0,0,0] 0	[0,1,0,0,0] 4.2	[0,0,1,0,0] 8.3	[0,0,0,1,0] 16.7	[0,0,0,0,1] 33.4
c_5	[1,0,0,0,0] 0	[0,1,0,0,0] 4.1	[0,0.47,0.53,0,0] 4.1	[0,0,0.41,0.59,0] 4.1	[0,0,0,0.33,0.67] 5.4
c_6	[1,0,0,0,0] 0	[0,1,0,0,0] 6	[0,0,1,0,0] 7.4	[0,0,0.44,0.56,0] 12	[0,0,0.32,0.52,0.16] 13.6

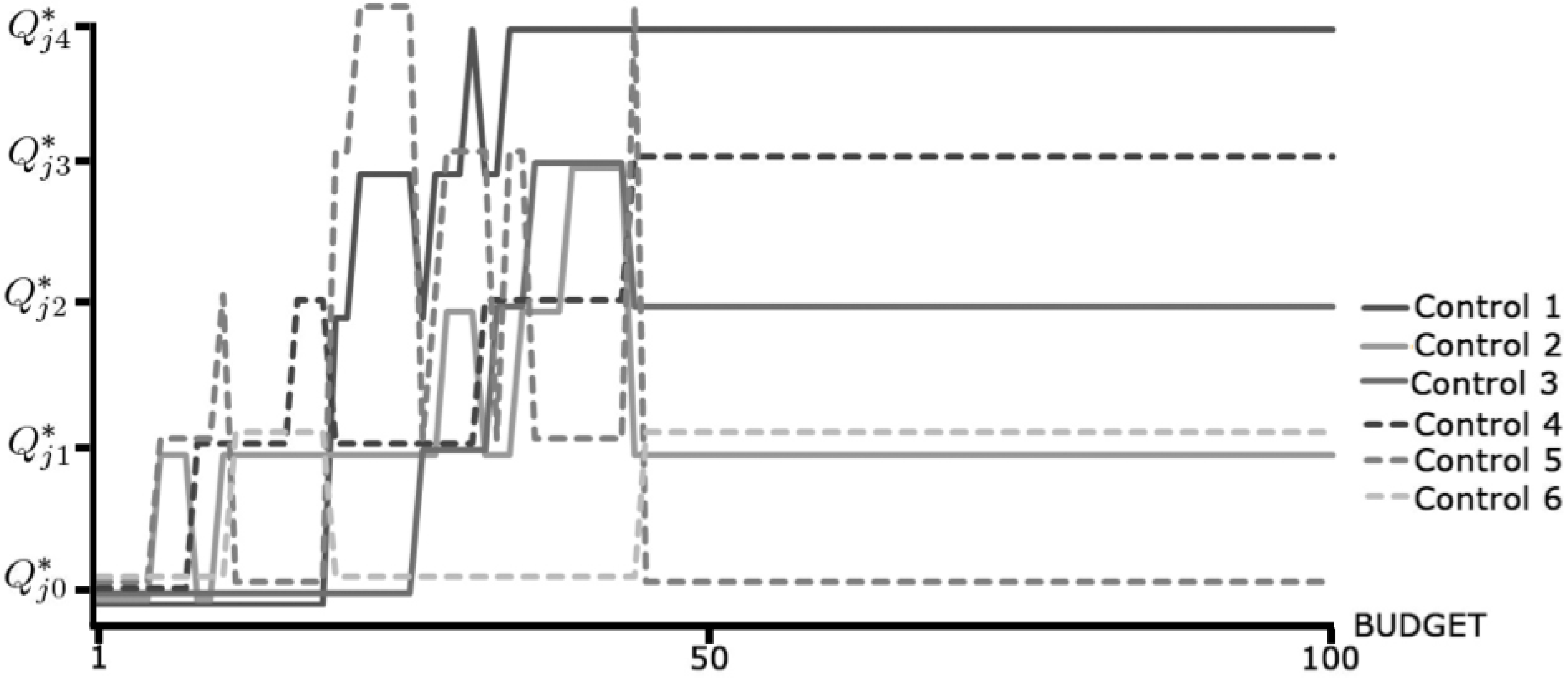


Level	$t(4,1)$	$t(4,2)$	$t(4,3)$	$t(9,1)$	$t(9,2)$	$t(9,3)$	$t(11,1)$	$t(11,2)$	$t(11,3)$	Solution	Implementation Cost
0	-8.75	-10.5	-12.25	-6.45	-7.5	-8.55	-8.75	-10.5 -	-12.25	[1,0,0,0,0]	0
1	-4.894	-5.988	-7.081	-3.456	-4.113	-4.769	-4.894	-5.988 -	7.081	[0,1,0,0,0]	4.1
2	-5.494	-6.588	-5.6	-4.056	-4.713	-4.12	-5.494	-6.588 -	-5.6	[0,0.47,0.53,0,0]	4.1
3	-6.094	-5.5	-6.2	-4.656	-4.3	-4.72	-6.094	-5.5 -	-6.2	[0,0,0.41,0.59,0]	4.1
4	-5.5	-6.2	-5.859	-4.58	-5.0	-4.796	-5.5	-6.2 -	-5.859	[0,0,0,0.33,0.67]	5.4

Results (II)

Knapsack Results

- Results for all budget levels using the organisation profile:
  - Risk Profile = [0.8, 0.1, 0.1]
  - Indirect Cost Profile = [0.5, 0.25, 0.25]
  - Threat Profile = [0.5, 0.5]



Results (III)

Case 1: Budget 17

- Optimal Solution - [0, 1, 0, 2, 0, 1] with a cost of 16.102.
  - With the given budget, Account Monitoring and Control (c_1) software should not be purchased, nor should system administrators spend time on activities to this control.
  - The organization must implement the Continuous Vulnerability Assessment and Remediation (c_2) control by purchasing a vulnerability scanner and patch management software. Additionally system administrators measuring the delay in patching new vulnerabilities and audit the results of vulnerability scans at all network depths infrequently (for example, once per month).
  - The decision tool does not recommend the implementation of specific Malware Defences (c_3) given the available budget.
  - The security manager is advised to schedule regular (e.g., twice a year) system-wide Penetration Tests and Red Team Exercises (c_4), with system updates being performed based on the results of the exercise.
  - The tool does not recommend the implementation of the Controlled Use of Administrative Privileges (c_5) control which means that neither enterprise password manager software should be purchased nor any password renewal policy should be enforced.
  - The tool recommends the implementation of the Data Loss Prevention (c_6) control system-wide and at a basic level (e.g., integrated services router with security, VPN).

Results (IV)

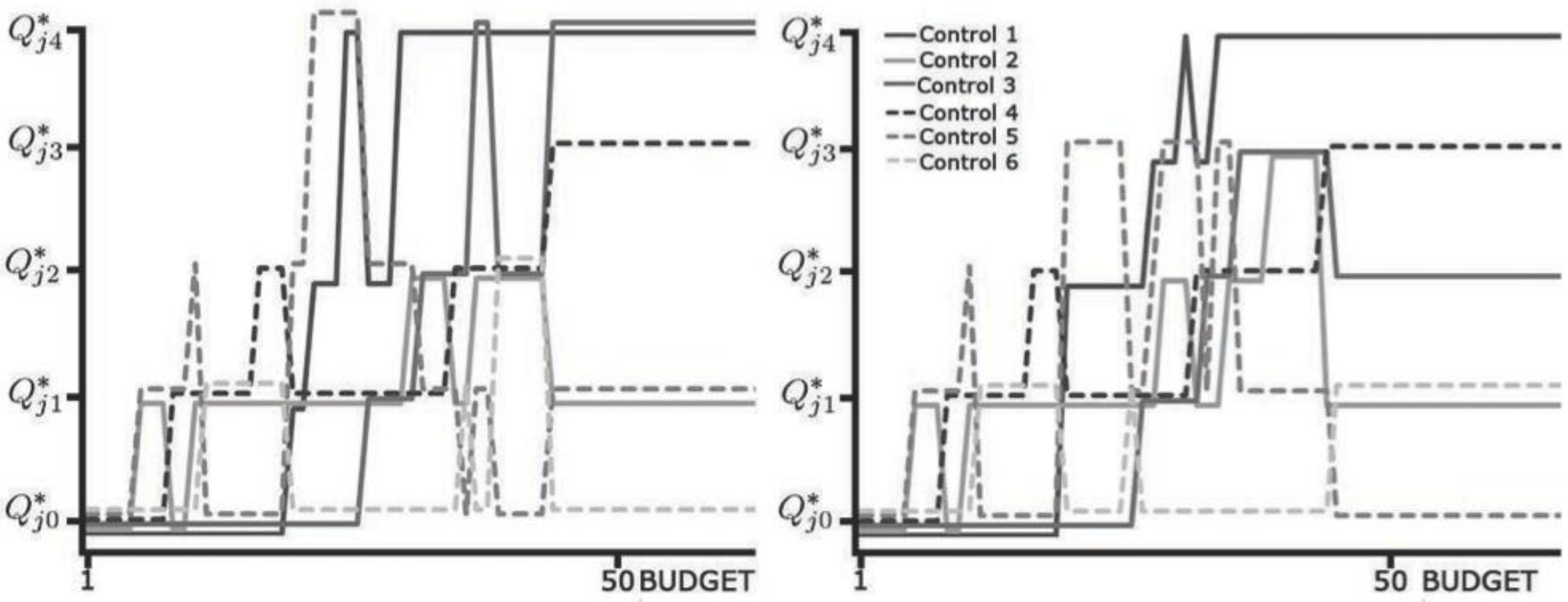
Case 2: Budget 28

- Optimal Solution - [3, 1, 1, 1, 2, 0] with a cost of 27.80.
  - Implementation of Account Monitoring and Control (c_1) at a basic level (e.g., control built into OS and manually review all accounts or set files/folders auditing properties) in all devices in DMZ; in 63% of the devices in Middleware; and in 40% of the devices in Private Network. The control must be also implemented at an advanced level (e.g., vulnerability scanner and patch management software) in 37% of the devices in Middleware and 60% of the devices in Private Network.
  - System-wide Continuous Vulnerability Assessment and Remediation (c_2) must be implemented infrequently (e.g., once per month).
  - System-wide Malware Defences (c_3) must be implemented at a basic level (e.g., free anti-malware with manual scheduled scans and database updates).
  - Penetration Tests and Red Team Exercises (c_4) to be undertaken infrequently (e.g., once per year).
  - Controlled Use of Administrative Privileges (c_5) to be implemented at a basic level (e.g., using an enterprise password manager software) with 47% of the devices to change passwords infrequently (e.g., once per year) and 53% regularly (e.g., every 4 months).
  - The purchase of a Data Loss Prevention control (c_6) is not recommended.

Results (V)

- Results for organisation profile:
  - Risk Profile = [0.6, 0.4, 0.0]
  - Indirect Cost Profile = [0.5, 0.25, 0.25]
  - Threat Profile = [0.5, 0.5]

- Results for organisation profile:
  - Risk Profile = [0.8, 0.1, 0.1]
  - Indirect Cost Profile = [0.3, 0.1, 0.6]
  - Threat Profile = [0.5, 0.5]



Conclusions

Summary

- Created a Decision Support methodology for the optimal allocation of cyber security budgets
- Uses an organisation profile to support a transition in cyber security decision making from system knowledge to business knowledge
- Presents a small case study showing the potential of the model

Future Work

- Highlight the mathematical elements and critical conditions of the model
- Improve the understanding of the interactions between controls
- Improve the scale and detail of the controls, increasing the size of the case study through work with our industrial partners